

REMARKS

A review of the claims indicates that:

A) Claims 2—5, 7, 8, 11, 13, 14, 16, 19, 20, 22—25, and 28 remain in their original form.

B) Claims 1, 6, 9, 10, 12, 15, 18, 21, 26, 29—33 and 35 are currently amended.

E) Claims 17, 27 and 34 are currently cancelled.

In view of the following remarks, Applicant respectfully requests reconsideration of the rejected claims.

35 U.S.C. §102 Rejections

Applicant submits that the Office has failed to establish a *prima facie* case of anticipation and respectfully traverses the Office's rejections. However, before discussing the substance of the Office's rejections, a section entitled "The §102 Standard" is provided and will be used in addressing the Office's rejections.

The §102 Standard

According to the MPEP §2131, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. The identical invention must be shown in as complete detail as is contained in the claim.

Anticipation is a legal term of art. The applicant notes that in order to provide a valid finding of anticipation, several conditions must be met: (i) the reference must include every element of the claim within the four corners of the reference (see MPEP §2121); (ii) the elements must be set forth as they are recited in the claim (see MPEP §2131); (iii) the teachings of the reference cannot be modified (see MPEP §706.02, stating that "No question of obviousness is present"

1 in conjunction with anticipation); and (iv) the reference must enable the invention
2 as recited in the claim (see MPEP §2121.01). Additionally, (v) these conditions
3 must be simultaneously satisfied.

4 The §102 rejection of claims 1—16, 18—26, 28—33 and 35, as
5 amended, is believed to be in error. Specifically, the PTO and Federal
6 Circuit provide that §102 anticipation requires that each and every element
7 of the claimed invention be disclosed in a single prior art reference. *In re*
8 *Spada*, 911 F.2d 705, 15 USPQ2d 1655 (Fed. Cir. 1990). The corollary of
9 this rule is that the absence from a cited §102 reference of any claimed
10 element negates the anticipation. *Kloster Speedsteel AB, et al. v. Crucible,*
11 *Inc., et al.*, 793 F.2d 1565, 230 USPQ 81 (Fed. Cir. 1986).

12 The applicant notes the requirements of MPEP §2131, which states
13 “to anticipate a claim, the reference must teach every element of the claim.”
14 This MPEP section further states that “A claim is anticipated only if each
15 and every element as set forth in the claim is found, either expressly or
16 inherently described, in a single prior art reference.” *Verdegaal Bros. v.*
17 *Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053
18 (Fed. Cir. 1987). “The identical invention must be shown in as complete
19 detail as is contained in the ... claim.” *Richardson v. Suzuki Motor Co.*, 868
20 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements
21 must be arranged as required by the claim, but this is not an ipsissimis verbis
22 test, i.e., identity of terminology is not required. *In re Bond*, 910 F.2d 831,
23 15 USPQ2d 1566 (Fed. Cir. 1990)."
24
25

Traversal of the §102 Rejections

Claims 1—35 were rejected under §102 as being anticipated by U.S. Patent No. 6,711,677, hereinafter “Wiegley.” In response, the Applicant respectfully traverses the rejection.

Claim 1 recites a printer device comprising:

- a data input device for receiving an encrypted digital document file;
- a decryption algorithm for decrypting said received document file;
- a controller for controlling printing of an image of data contained in said received document file, **wherein said controller operates to read a quantity permission data content of said document file, said quantity permission data specifying a number of authorized copies of said document file to be printed;** and
- a printer mechanism for printing a physical copy of said document file;
- wherein said controller operates to control printing of a predetermined quantity of said physical copy, and after printing of said physical copy, automatically deletes said electronic document file from said memory.

Claim 1 has been amended to include elements originally recited in Claim 6, as seen in bold, above.

The Wiegley reference fails to disclose a controller configured to “read a quantity permission data content of said document file, said quantity permission data specifying a number of authorized copies of said document file to be printed”. Accordingly, Wiegley does not disclose aspects recited by Claim 1.

In formulating a rejection of Claim 6 (relevant here, since the amendment to Claim 1 included material from Claim 6) the Patent Office points to column 4, lines 30—46. The Applicant respectfully disagrees with this characterization of this passage in Wiegley.

1 Referring to column 4, lines 30—46, Wiegley discusses public and private
2 keys, and use of an authenticity certificate (lines 30—37). The authenticity
3 certificate includes data on the printer, including its name, the name of the
4 authenticating authority and the authority's signature (lines 37—42). A computer
5 sending a print job can verify the certificate as a step in a security system, thereby
6 adding a measure of security to help prevent printer impersonations (lines 42—
7 46). Thus, the passage cited by the Patent Office fails to disclose "a number of
8 authorized copies" of a document file to be printed.

9 Therefore, at least this element recited in the Applicant's Claim 1, as
10 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
11 respectfully requests that the rejection to Claim 1, as amended, be removed.

12 **Claims 2—8** depend from Claim 1 and are allowable due to their
13 dependence from an allowable base claim. These claims are also allowable for
14 their own recited features that, in combination with those recited in Claim 1, are
15 neither disclosed nor suggested in references of record, either singly or in
16 combination with one another.

17 **Claim 9** recites a printer device comprising:

- 18 • a data input device for receiving an encrypted digital document file;
- 19 • a decryption algorithm for decrypting said received document file;
- 20 • a controller for controlling printing of an image of data contained in
21 said received document file, **wherein said controller operates to**
22 **read a quantity permission data content of said document file,**
23 **said quantity permission data specifying a number of authorized**
24 **copies of said document file to be printed; and**
- 25 • a printer mechanism for printing a physical copy of said document
file, wherein said controller operates to check a unique device
identification data contained in said document file with a stored
unique device identification data of said printer device, and provided
a successful match is found, print said physical copy of said
document file; and

- if said received unique device identifier differs from said stored unique device identifier data, said controller operates to delete said document file without printing a physical copy of said document file.

Claim 9 has been amended in a manner similar to that of Claim 1. Therefore, the arguments traversing the rejection of Claim 1 are incorporated herein by reference. In view of these arguments, the Applicant submits that the elements recited in Claim 9, as amended, is not disclosed by the prior art of record. Accordingly, the Applicant respectfully requests that the rejection to Claim 9, as amended, be removed.

Claim 10 recites a computer entity configured for sending secure encrypted document files, said computer entity comprising:

- a data processor;
- a memory;
- an encryption algorithm capable of encrypting a document file;
- a device selector for selecting a said uniquely identifiable recipient device;
- a file selector for selecting a document file;
- a stored list of a set of authorized recipient devices, each said recipient device identified by a unique device identifier data inaccessibly embedded within said computer entity.
- wherein said computer entity operates to:
 - select at least one document file;
 - select at least one said uniquely identifiable recipient device to send said document to;
 - encrypt said document files; and
 - address said at least one document file to said selected uniquely identified recipient device; and
- **a user interface capable of displaying a history list of document files sent, said history list comprising:**
 - **data describing a document file sent;**
 - **data describing at least one said recipient device to which said document file has been sent; and**
 - **data describing a number of copies of documents said recipient device is authorized to print from said received document file.**

1 Claim 10 has been amended to include elements originally recited in Claim
2 12, as seen in bold, above.

3 The Wiegley reference fails to disclose “a number of copies of documents
4 said recipient device is authorized to print from said received document file” as
5 recited by Claim 10, as amended (last 3 lines). Therefore, Wiegley does not
6 disclose elements recited in the claim.

7 In formulating a rejection of Claim 12 (relevant here, since the amendment
8 to Claim 10 included material from Claim 12) the Patent Office points to column
9 4, lines 30—46. The Applicant respectfully disagrees with this characterization of
10 this passage in Wiegley.

11 Referring to column 4, lines 30—46, Wiegley discusses public and private
12 keys, and use of an authenticity certificate (lines 30—37). The authenticity
13 certificate includes data on the printer, including its name, the name of the
14 authenticating authority and the authority’s signature (lines 37—42). A computer
15 sending a print job can verify the certificate as a step in a security system, thereby
16 adding a measure of security to help prevent printer impersonations (lines 42—
17 46). Thus, the passage cited by the Patent Office fails to disclose, “data describing
18 a number of copies of documents said recipient device is authorized to print from
19 said received document file”.

20 Therefore, at least this element recited in the Applicant’s Claim 10, as
21 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
22 respectfully requests that the rejection to Claim 10, as amended, be removed.
23
24
25

1 **Claims 11—14** depend from Claim 10 and are allowable due to their
2 dependence from an allowable base claim. These claims are also allowable for
3 their own recited features that, in combination with those recited in Claim 10, are
4 neither disclosed nor suggested in references of record, either singly or in
5 combination with one another.

6 **Claim 15** recites a distributed secure document printing system, said
7 system comprising:

- 8 • at least one sending computer entity, capable of sending an
9 encrypted electronic document file, said document file having an
10 encrypted data content, and a unique device identifier data
11 identifying a recipient printer device to which said document file is
12 intended to be printed by; and
- 13 • at least one recipient printer device, said recipient printer device
14 capable of receiving said encrypted document file, establishing that
15 said document file is intended for said recipient printer device,
16 decrypting and printing said document file, and automatically
17 deleting said electronic document file after printing a physical copy
18 of a document from said document file;
- 19 • wherein said recipient printer device is configured to send a
20 **confirmation message back to said sending computer entity,**
21 **confirming receipt of said document file, and confirming**
22 **printing of a specified permitted number of copies of said**
23 **document file.**

24 Claim 15 has been amended to include elements originally recited in Claim
25 17, as seen in bold, above.

 The Wiegley reference fails to disclose a printing device configured to send
“a confirmation message back to said sending computer entity, confirming receipt
of said document file, and confirming printing of a specified permitted number of
copies of said document file” as recited by Claim 15, as amended (last several
lines).

1 In formulating a rejection of Claim 17 (relevant here, since the amendment
2 to Claim 15 included material from Claim 17) the Patent Office points to column
3 4, lines 30—46. The Applicant respectfully disagrees with this characterization of
4 this passage in Wiegley.

5 Referring to column 4, lines 30—46, Wiegley discusses public and private
6 keys, and use of an authenticity certificate (lines 30—37). The authenticity
7 certificate includes data on the printer, including its name, the name of the
8 authenticating authority and the authority's signature (lines 37—42). A computer
9 sending a print job can verify the certificate as a step in a security system, thereby
10 adding a measure of security to help prevent printer impersonations (lines 42—
11 46). Thus, the passage cited by the Patent Office fails to disclose "a confirmation
12 message back to said sending computer entity, confirming receipt of said
13 document file, and confirming printing of a specified permitted number of copies
14 of said document file".

15 Therefore, at least this element recited in the Applicant's Claim 15, as
16 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
17 respectfully requests that the rejection to Claim 15, as amended, be removed.

18 **Claim 16** depends from Claim 15 and is allowable due to its dependence
19 from an allowable base claim. This claim is also allowable for its own recited
20 features that, in combination with those recited in Claim 15, are neither disclosed
21 nor suggested in references of record, either singly or in combination with one
22 another.

23
24 **Claim 18** recites a method of securely communicating an electronic
25 document file over a network, said method comprising the steps of:

- encrypting said document file;
- specifying a recipient device for sending said document file to, said recipient device being uniquely identifiable by a unique device identifier data;
- attaching said unique identifier data to said document file;
- sending said document file in encrypted format to said intended recipient device;
- receiving said transmitted document file and decrypting said document file;
- reading said unique device identifier data of said document file.
- if said unique device identifier data of said document file corresponds to a unique device identifier data of said recipient device, printing a physical copy of said document file;
- if said unique device identifier data of said document file does not correspond with said unique device identifier data of said recipient device, deleting said received document file without printing a physical copy of said document file; and
- **sending, from said recipient device, a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file.**

Claim 18 has been amended to include a version of elements originally recited in Claim 17, as seen in bold, above.

The Wiegley reference fails to disclose sending “a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file” as recited by Claim 18, as amended (last several lines).

In formulating a rejection of Claim 17 (relevant here, since the amendment to Claim 18 included material from Claim 17) the Patent Office points to column 4, lines 30—46. The Applicant respectfully disagrees with this characterization of this passage in Wiegley.

1 Referring to column 4, lines 30—46, Wiegley discusses public and private
2 keys, and use of an authenticity certificate (lines 30—37). The authenticity
3 certificate includes data on the printer, including its name, the name of the
4 authenticating authority and the authority's signature (lines 37—42). A computer
5 sending a print job can verify the certificate as a step in a security system, thereby
6 adding a measure of security to help prevent printer impersonations (lines 42—
7 46). Thus, the passage cited by the Patent Office fails to disclose "a confirmation
8 message back to said sending computer entity, confirming receipt of said
9 document file, and confirming printing of a specified permitted number of copies
10 of said document file".

11 Therefore, at least this element recited in the Applicant's Claim 18, as
12 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
13 respectfully requests that the rejection to Claim 18, as amended, be removed.

14 **Claims 19—20** depend from Claim 18 and are allowable due to their
15 dependence from an allowable base claim. These claims are also allowable for
16 their own recited features that, in combination with those recited in Claim 18, are
17 neither disclosed nor suggested in references of record, either singly or in
18 combination with one another.

19 **Claim 21** recites a method of secure printing of a received document file,
20 said method comprising the steps of:

- 21 • receiving said document file in encrypted format at a receiving
22 device;
- 23 • decrypting said document file;
- 24 • reading a unique device identifier data identifying a recipient device
25 for which said document file is intended;
- comparing said unique device identifier data with a locally stored
device identifier data stored at said receiving device;

- 1 • if said received unique device identifier data corresponds with said
2 locally stored device identifier data, printing at least one physical
3 copy of said document file; and
- 4 • if said received unique device identifier data differs from said stored
5 unique device identifier data, deleting said document file; and
- 6 • **sending, from said recipient device, a confirmation message back**
7 **to said sending computer entity, confirming receipt of said**
8 **document file, and confirming printing of a specified permitted**
9 **number of copies of said document file.**

10 Claim 21 has been amended to include a version of elements originally
11 recited in Claim 17, as seen in bold, above.

12 The Wiegley reference fails to disclose sending “a confirmation message
13 back to said sending computer entity, confirming receipt of said document file,
14 and confirming printing of a specified permitted number of copies of said
15 document file” as recited by Claim 18, as amended (last several lines).

16 In formulating a rejection of Claim 17 (relevant here, since the amendment
17 to Claim 21 included material from Claim 17) the Patent Office points to column
18 4, lines 30—46. The Applicant respectfully disagrees with this characterization of
19 this passage in Wiegley.

20 Referring to column 4, lines 30—46, Wiegley discusses public and private
21 keys, and use of an authenticity certificate (lines 30—37). The authenticity
22 certificate includes data on the printer, including its name, the name of the
23 authenticating authority and the authority’s signature (lines 37—42). A computer
24 sending a print job can verify the certificate as a step in a security system, thereby
25 adding a measure of security to help prevent printer impersonations (lines 42—
46). Thus, the passage cited by the Patent Office fails to disclose “a confirmation
message back to said sending computer entity, confirming receipt of said

1 document file, and confirming printing of a specified permitted number of copies
2 of said document file”.

3 Therefore, at least this element recited in the Applicant’s Claim 21, as
4 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
5 respectfully requests that the rejection to Claim 21, as amended, be removed.

6 **Claims 22—25** depend from Claim 21 and are allowable due to their
7 dependence from an allowable base claim. These claims are also allowable for
8 their own recited features that, in combination with those recited in Claim 21, are
9 neither disclosed nor suggested in references of record, either singly or in
10 combination with one another.

11 **Claim 26** recites a method of sending a document file for printing by a
12 specified authorized recipient printing device, said method comprising the steps
13 of:

- 14 • selecting a content of said document file;
- 15 • encrypting said content;
- 16 • attaching a unique device identifier data, identifying a recipient
17 device to which said document file is to be sent;
- 18 • sending said document file to said recipient device; and
- 19 • **adding a permitted quantity data to said document file, said
20 permitted quantity data specifying a permitted number of copies
21 of said document file which can be printed.**

22 Claim 26 has been amended to include a version of elements originally
23 recited in Claim 27, as seen in bold, above.

24 The Wiegley reference fails to disclose “adding a permitted quantity data to
25 said document file, said permitted quantity data specifying a permitted number of
copies of said document file which can be printed” as recited by Claim 18, as
amended (last several lines).

1 In formulating a rejection of Claim 27 (relevant here, since the amendment
2 to Claim 26 included material from Claim 27) the Patent Office points to column
3 4, lines 30—46. The Applicant respectfully disagrees with this characterization of
4 this passage in Wiegley.

5 Referring to column 4, lines 30—46, Wiegley discusses public and private
6 keys, and use of an authenticity certificate (lines 30—37). The authenticity
7 certificate includes data on the printer, including its name, the name of the
8 authenticating authority and the authority's signature (lines 37—42). A computer
9 sending a print job can verify the certificate as a step in a security system, thereby
10 adding a measure of security to help prevent printer impersonations (lines 42—
11 46). Thus, the passage cited by the Patent Office fails to disclose “adding a
12 permitted quantity data to said document file, said permitted quantity data
13 specifying a permitted number of copies of said document file which can be
14 printed”.

15 Therefore, at least this element recited in the Applicant's Claim 26, as
16 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
17 respectfully requests that the rejection to Claim 26, as amended, be removed.

18 **Claim 28** depends from Claim 26 and is allowable due to its dependence
19 from an allowable base claim. This claim is also allowable for its own recited
20 features that, in combination with those recited in Claim 26, are neither disclosed
21 nor suggested in references of record, either singly or in combination with one
22 another.

1 **Claim 29** recites a computer entity comprising a data processor, a data
2 storage device, a printer port, and having an attached printer device, said computer
3 entity comprising:

- 4 • a module for decrypting an encrypted document file;
- 5 • a unique device identifier for identifying said computer entity;
- 6 • wherein said computer entity operates to:
 - 7 • receive a document file in encrypted format;
 - 8 • decrypt said document;
 - 9 • extract a unique device identifier data from said document;
 - 10 • compare said extracted unique identifier data with said unique
11 device identifier of said computer entity;
 - 12 • if a match is found between said received unique device
13 identifier data of said document and said unique identifier of said
14 computer entity, send a said document file for printing by said
15 attached printer device; and
 - 16 • after sending said document to said printer device, delete said
17 document file from said computer entity; and
- 18 • **adding a permitted quantity data to said document file, said
19 permitted quantity data specifying a permitted number of copies
20 of said document file which can be printed.**

21 Claim 29 has been amended to include a version of elements originally
22 recited in Claim 27, as seen in bold, above.

23 The Wiegley reference fails to disclose “adding a permitted quantity data to
24 said document file, said permitted quantity data specifying a permitted number of
25 copies of said document file which can be printed” as recited by Claim 18, as
amended (last several lines).

 In formulating a rejection of Claim 27 (relevant here, since the amendment
to Claim 29 included material from Claim 27) the Patent Office points to column
4, lines 30—46. The Applicant respectfully disagrees with this characterization of
this passage in Wiegley.

 Referring to column 4, lines 30—46, Wiegley discusses public and private
keys, and use of an authenticity certificate (lines 30—37). The authenticity

1 certificate includes data on the printer, including its name, the name of the
2 authenticating authority and the authority's signature (lines 37—42). A computer
3 sending a print job can verify the certificate as a step in a security system, thereby
4 adding a measure of security to help prevent printer impersonations (lines 42—
5 46). Thus, the passage cited by the Patent Office fails to disclose “adding a
6 permitted quantity data to said document file, said permitted quantity data
7 specifying a permitted number of copies of said document file which can be
8 printed”.

9 Therefore, at least this element recited in the Applicant's Claim 29, as
10 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
11 respectfully requests that the rejection to Claim 29, as amended, be removed.

12 **Claim 30** recites a method of secure printing of a received document file,
13 said method comprising the steps of:

- 14 • receiving said document file in encrypted format;
- 15 • reading a unique device identifier data identifying a recipient device
16 for which said document file is intended;
- 17 • comparing said unique device identifier data with a locally stored
18 identifier data corresponding to a local computer entity device;
- 19 • if said locally stored identifier data differs from said unique device
20 identifier data identifying said recipient device for which said
document file is intended, deleting said document file without
printing any physical copies of said document file; and
- 21 • **printing a number of physical copies of said document file,**
22 **corresponding to a permitted quantity defined in said document**
23 **file.**

24 Claim 30 has been amended to include a version of elements originally
25 recited in Claim 16, as seen in bold, above.

1 The Wiegley reference fails to disclose “printing a number of physical
2 copies of said document file, corresponding to a permitted quantity defined in said
3 document file” as recited by Claim 16, as amended (last several lines).

4 In formulating a rejection of Claim 16 (relevant here, since the amendment
5 to Claim 30 included material from Claim 16) the Patent Office points to column
6 4, lines 30—46. The Applicant respectfully disagrees with this characterization of
7 this passage in Wiegley.

8 Referring to column 4, lines 30—46, Wiegley discusses public and private
9 keys, and use of an authenticity certificate (lines 30—37). The authenticity
10 certificate includes data on the printer, including its name, the name of the
11 authenticating authority and the authority’s signature (lines 37—42). A computer
12 sending a print job can verify the certificate as a step in a security system, thereby
13 adding a measure of security to help prevent printer impersonations (lines 42—
14 46). Thus, the passage cited by the Patent Office fails to disclose “printing a
15 number of physical copies of said document file, corresponding to a permitted
16 quantity defined in said document file”.

17 Therefore, at at least this element recited in the Applicant’s Claim 30, as
18 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
19 respectfully requests that the rejection to Claim 30, as amended, be removed.

20 **Claim 31** recites a method of secure printing of a received document file,
21 said method comprising the steps of:

- 22 • receiving said document file in encrypted format;
- 23 • reading a unique device identifier data identifying a recipient device
24 for which said document file is intended;
- 25 • comparing said unique device identifier data with a locally stored
device identifier data;

- reading a permitted quantity data describing a permitted quantity of copies of said document file;
- if said received unique device identifier data corresponds with said locally stored device identifier data, printing said permitted quantity of copies of said document file; and
- **printing a number of physical copies of said document file, corresponding to a permitted quantity defined in said document file.**

Claim 31 has been amended to include a version of elements originally recited in Claim 16, as seen in bold, above.

The Wiegley reference fails to disclose sending “printing a number of physical copies of said document file, corresponding to a permitted quantity defined in said document file” as recited by Claim 16, as amended (last several lines).

In formulating a rejection of Claim 16 (relevant here, since the amendment to Claim 31 included material from Claim 16) the Patent Office points to column 4, lines 30—46. The Applicant respectfully disagrees with this characterization of this passage in Wiegley.

Referring to column 4, lines 30—46, Wiegley discusses public and private keys, and use of an authenticity certificate (lines 30—37). The authenticity certificate includes data on the printer, including its name, the name of the authenticating authority and the authority’s signature (lines 37—42). A computer sending a print job can verify the certificate as a step in a security system, thereby adding a measure of security to help prevent printer impersonations (lines 42—46). Thus, the passage cited by the Patent Office fails to disclose “printing a number of physical copies of said document file, corresponding to a permitted quantity defined in said document file”.

1 Therefore, at least this element recited in the Applicant's Claim 31, as
2 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
3 respectfully requests that the rejection to Claim 31, as amended, be removed.

4 **Claim 32** recites a printer device comprising:

- 5 • a data input device for receiving an encrypted digital document file;
- 6 • a decryption algorithm for decrypting said received document file;
- 7 • a controller for controlling printing of an image of data contained in
8 said received document file; and
- 9 • a printer mechanism for printing a physical copy of said document
10 file,
- 11 • wherein said printer device locally stores a decryption key for
12 operating said decryption algorithm to decrypt said received
document file; and
- 13 • **wherein said printer device is configured to send a confirmation
14 message back to said sending computer entity, confirming
15 receipt of said document file, and confirming printing of a
16 specified permitted number of copies of said document file.**

17 Claim 32 has been amended to include elements originally recited in Claim
18 17, as seen in bold, above.

19 The Wiegley reference is silent about a printing device "configured to send
20 a confirmation message back to said sending computer entity, confirming receipt
21 of said document file, and confirming printing of a specified permitted number of
22 copies of said document file" as recited by Claim 32, as amended (last several
23 lines).

24 In formulating a rejection of Claim 17 (relevant here, since the amendment
25 to Claim 32 included material from Claim 17) the Patent Office points to column
4, lines 30—46. The Applicant respectfully disagrees with this characterization of
this passage in Wiegley.

1 Referring to column 4, lines 30—46, Wiegley discusses public and private
2 keys, and use of an authenticity certificate (lines 30—37). The authenticity
3 certificate includes data on the printer, including its name, the name of the
4 authenticating authority and the authority's signature (lines 37—42). A computer
5 sending a print job can verify the certificate as a step in a security system, thereby
6 adding a measure of security to help prevent printer impersonations (lines 42—
7 46). Thus, the passage cited by the Patent Office fails to disclose a printer
8 "configured to send a confirmation message back to said sending computer entity,
9 confirming receipt of said document file, and confirming printing of a specified
10 permitted number of copies of said document file".

11 Therefore, at least this element recited in the Applicant's Claim 32, as
12 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
13 respectfully requests that the rejection to Claim 32, as amended, be removed.

14 **Claim 33** recites a printer device comprising:

- 15 • a data input device for receiving a digital document file;
- 16 • a controller for controlling printing of an image of data contained in
17 said received document file; and
- 18 • a printer mechanism for printing a physical copy of said document
19 file,
- 20 • wherein said controller operates to compare a received unique
21 identifier data contained in said received document file with a
22 locally stored unique device identifier data stored at said printer
23 device and operates **to control printing of a predetermined
24 quantity of said physical copy, wherein said predetermined
25 quantity is specified in said received document file;**
- if said received unique identifier data matches said stored unique
device identifier, control printing of at least one said physical copy
of said document file; and
- if said received unique identifier data contained the said received
document file does not match said stored unique device identifier
data, to inhibit printing of any physical copies of said document file.

1 Claim 33 has been amended to include a version of elements originally
2 recited in Claim 16, as seen in bold, above.

3 The Wiegley reference fails to disclose sending “printing a number of
4 physical copies of said document file, corresponding to a permitted quantity
5 defined in said document file” as recited by Claim 16, as amended (last several
6 lines).

7 In formulating a rejection of Claim 16 (relevant here, since the amendment
8 to Claim 30 included material from Claim 16) the Patent Office points to column
9 4, lines 30—46. The Applicant respectfully disagrees with this characterization of
10 this passage in Wiegley.

11 Referring to column 4, lines 30—46, Wiegley discusses public and private
12 keys, and use of an authenticity certificate (lines 30—37). The authenticity
13 certificate includes data on the printer, including its name, the name of the
14 authenticating authority and the authority’s signature (lines 37—42). A computer
15 sending a print job can verify the certificate as a step in a security system, thereby
16 adding a measure of security to help prevent printer impersonations (lines 42—
17 46). Thus, the passage cited by the Patent Office fails to disclose “printing a
18 number of physical copies of said document file, corresponding to a permitted
19 quantity defined in said document file”.

20 Therefore, at least this element recited in the Applicant’s Claim 33, as
21 amended, is not disclosed by the prior art of record. Accordingly, the Applicant
22 respectfully requests that the rejection to Claim 33, as amended, be removed.

23 **Claim 35** recites a printer device comprising:

- 24 • a data input device for receiving an encrypted digital document file;
- 25

- a decryption algorithm for decrypting said received document files; a controller for controlling printing of an image of data contained in said received document file;
- a printer mechanism for printing a physical copy of said document file,
- wherein a decryption key is stored locally in said printer device for operating said decryption algorithm to decrypt said received document files;
- said controller operates to compare a received unique identifier data contained in said received document file with a locally stored unique device identifier data stored at said printer device;
- if said received unique identifier data matches said stored unique device identifier, control printing of at least one said physical copy of said document file; and
- if said received unique identifier data contained the said received document file does not match said stored unique device identifier data, to inhibit decryption of said document file and inhibit printing of any physical copies of said document file;
- wherein said printer device **is configured to send a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file.**

Claim 35 has been amended to include elements originally recited in Claim 17, as seen in bold, above.

The Wiegley reference fails to disclose a printing device sending “a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file” as recited by Claim 15, as amended (last several lines).

In formulating a rejection of Claim 17 (relevant here, since the amendment to Claim 35 included material from Claim 17) the Patent Office points to column 4, lines 30—46. The Applicant respectfully disagrees with this characterization of this passage in Wiegley.

Referring to column 4, lines 30—46, Wiegley discusses public and private keys, and use of an authenticity certificate (lines 30—37). The authenticity certificate includes data on the printer, including its name, the name of the authenticating authority and the authority's signature (lines 37—42). A computer sending a print job can verify the certificate as a step in a security system, thereby adding a measure of security to help prevent printer impersonations (lines 42—46). Thus, the passage cited by the Patent Office fails to disclose "a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file".

Therefore, at least this element recited in the Applicant's Claim 35, as amended, is not disclosed by the prior art of record. Accordingly, the Applicant respectfully requests that the rejection to Claim 35, as amended, be removed.

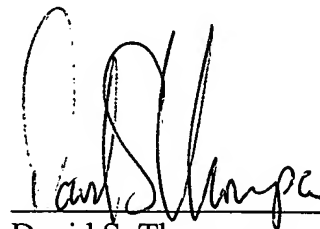
Conclusion

The Applicant submits that all of the claims are in condition for allowance and respectfully requests that a Notice of Allowability be issued. If the Office's next anticipated action is not the issuance of a Notice of Allowability, the Applicant respectfully requests that the undersigned attorney be contacted for the purpose of scheduling an interview.

Respectfully Submitted,

Dated: 12-20-2005

By:



David S. Thompson
Reg. No. 37,954
Attorney for Applicant

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

LEE & HAYES PLLC
Suite 500
421 W. Riverside Avenue
Spokane, Washington 99201
Telephone: 509-324-9256 x235
Facsimile: (509) 323-8979